FIG. 1
(PRIOR ART)

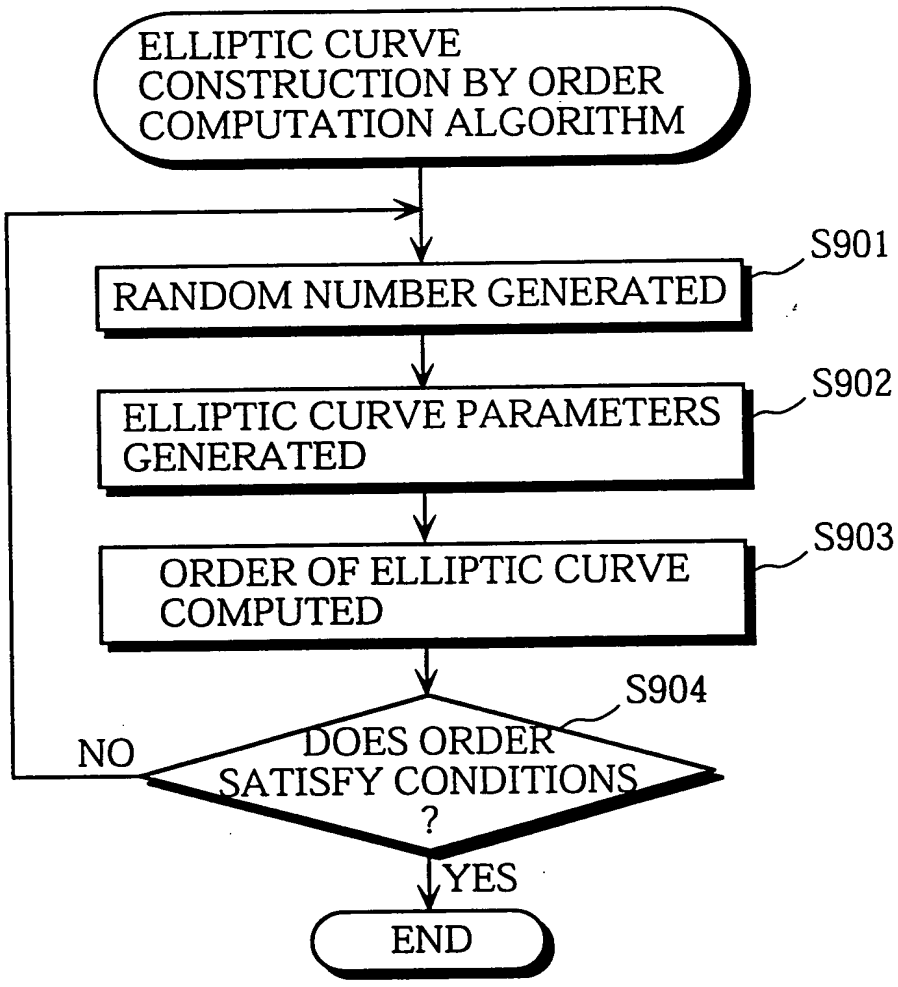


FIG. 2
(PRIOR ART)

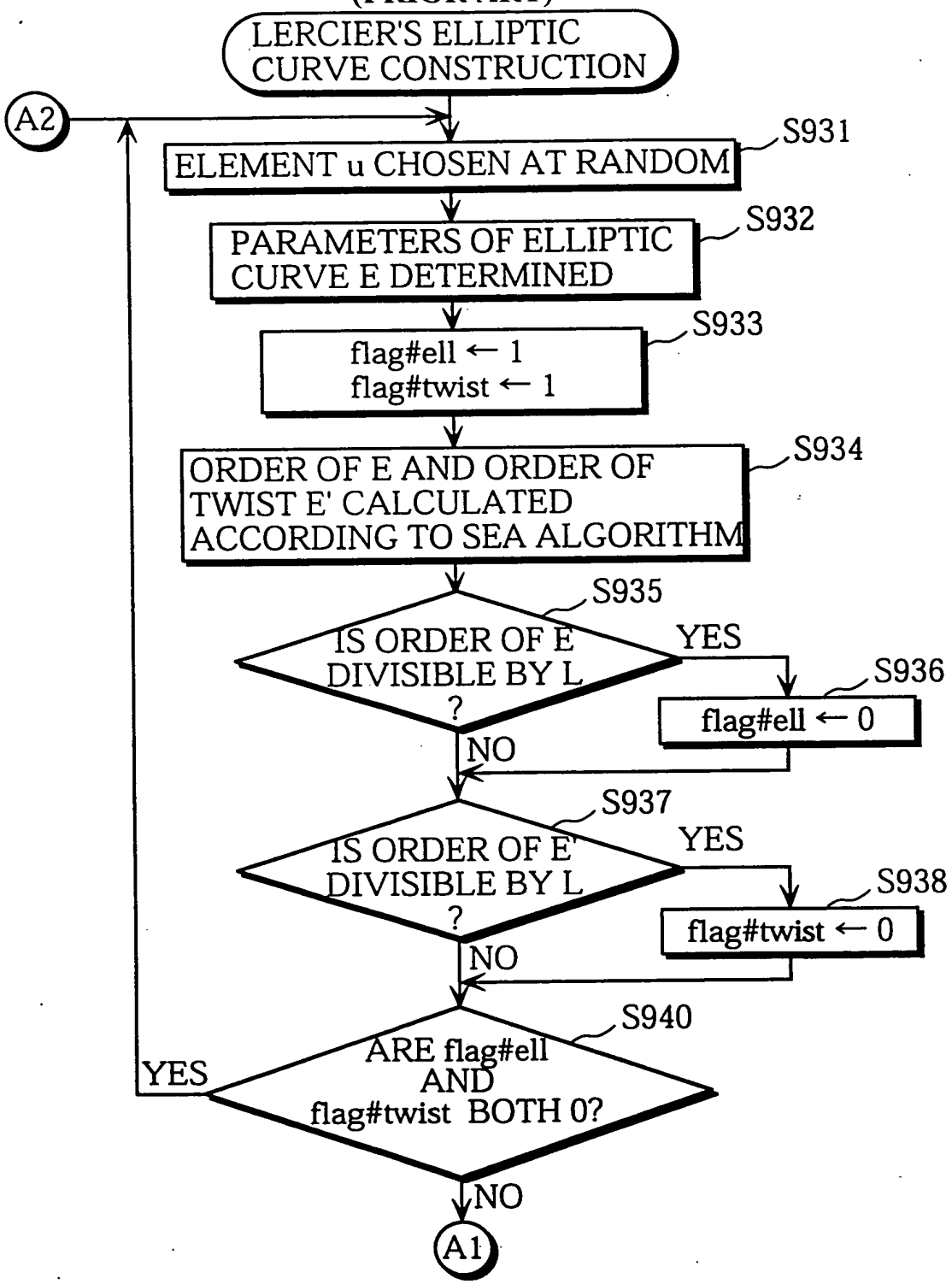


FIG. 3
(PRIOR ART)

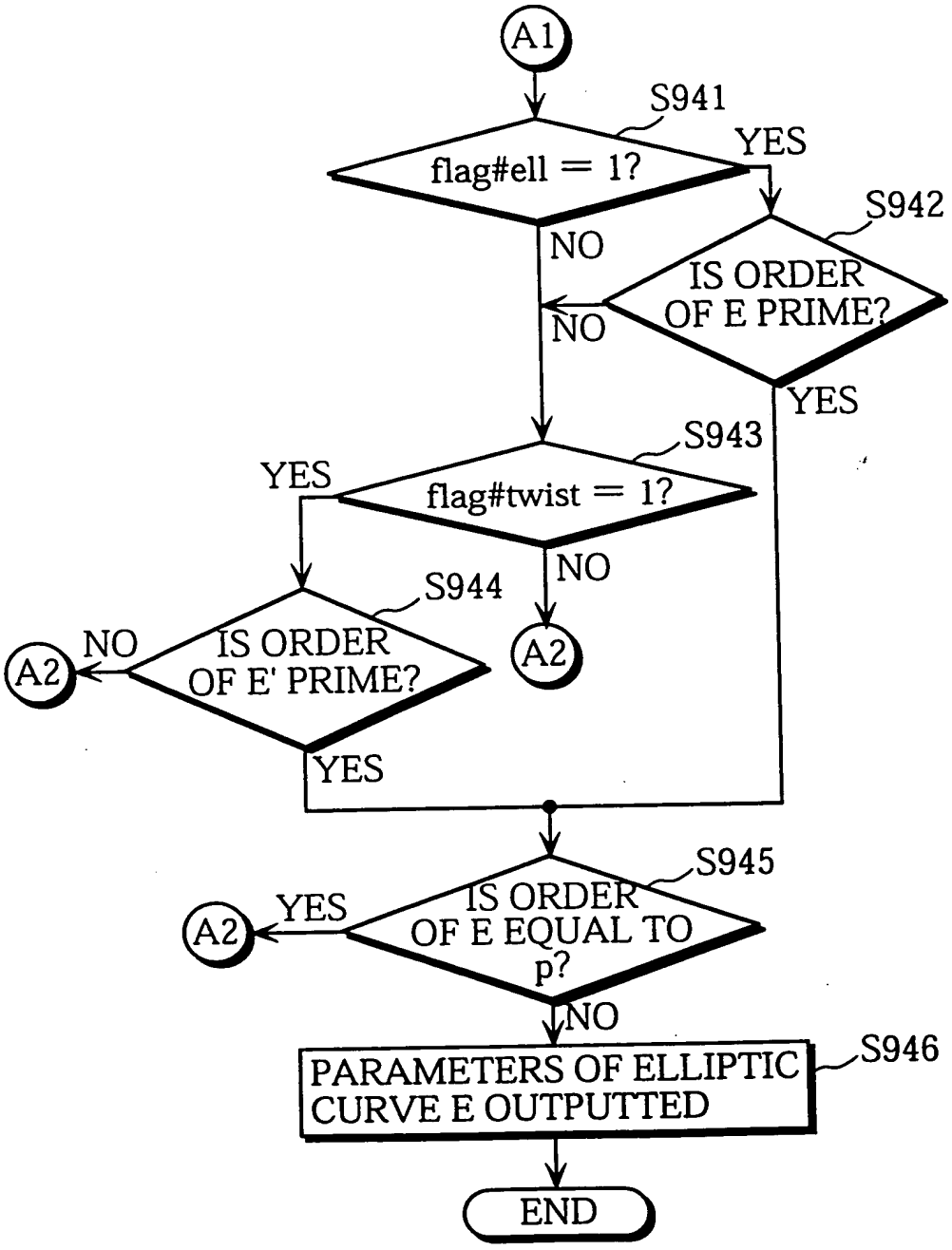


FIG. 4

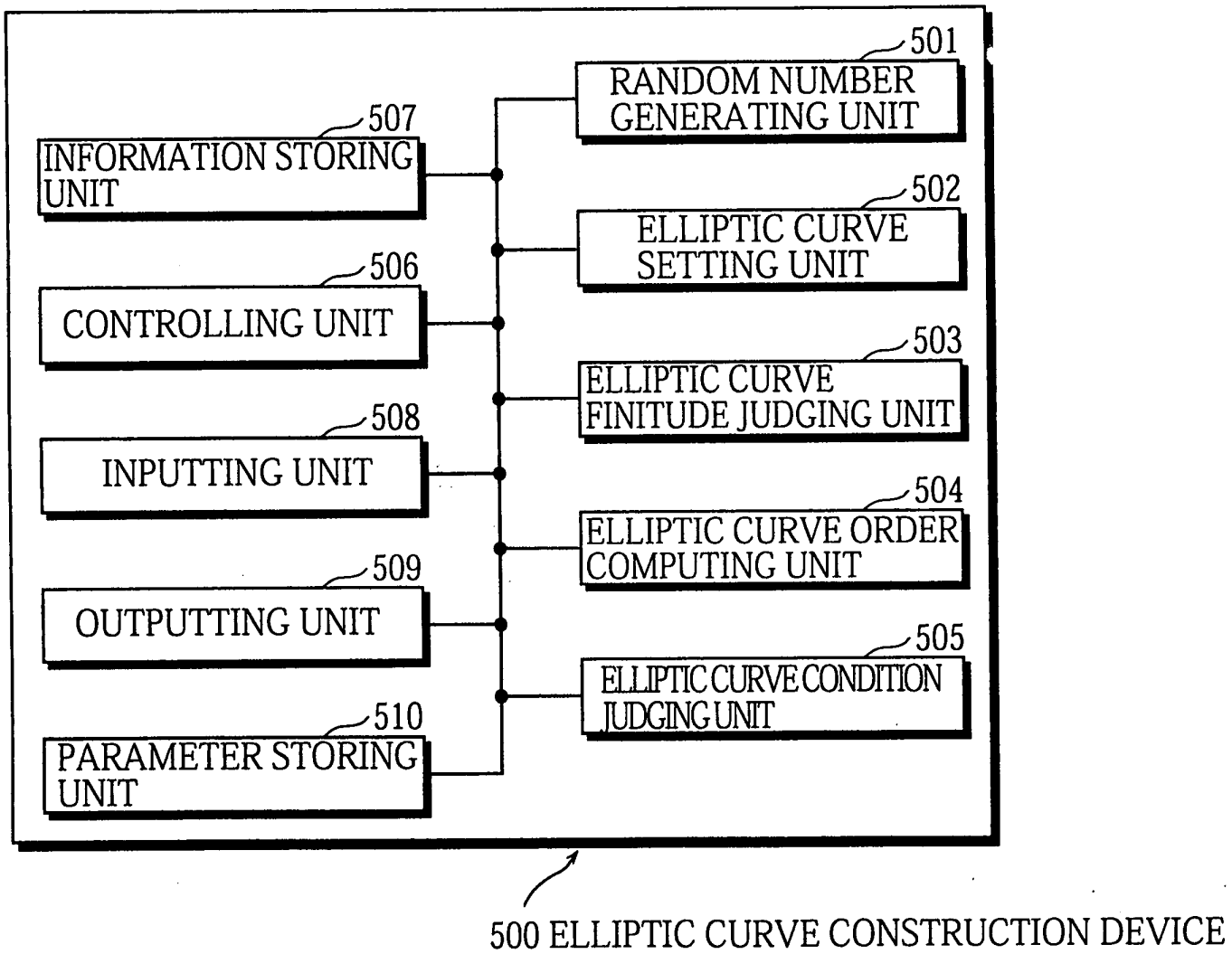

501
RANDOM NUMBER GENERATING UNIT
507
INFORMATION STORING UNIT
502
ELLIPTIC CURVE SETTING UNIT
506
CONTROLLING UNIT
503
ELLIPTIC CURVE FINITUDE JUDGING UNIT
508
INPUTTING UNIT
504
ELLIPTIC CURVE ORDER COMPUTING UNIT
509
OUTPUTTING UNIT
505
ELLIPTIC CURVE CONDITION JUDGING UNIT
510
PARAMETER STORING UNIT
500 ELLIPTIC CURVE CONSTRUCTION DEVICE

FIG. 5

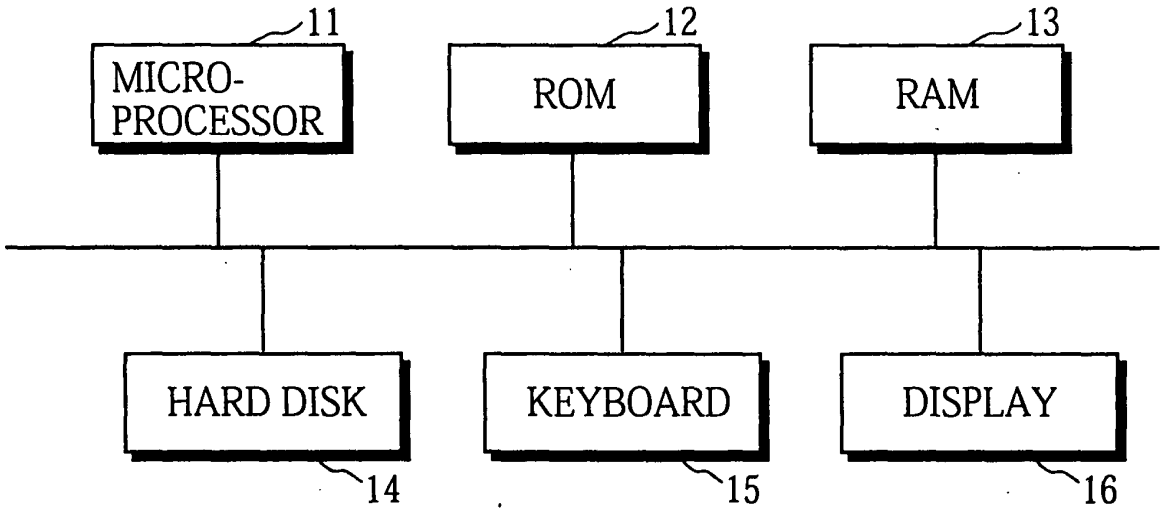

11
MICRO-
PROCESSOR
12
ROM
13
RAM
HARD DISK
14
KEYBOARD
15
DISPLAY
16

FIG. 6

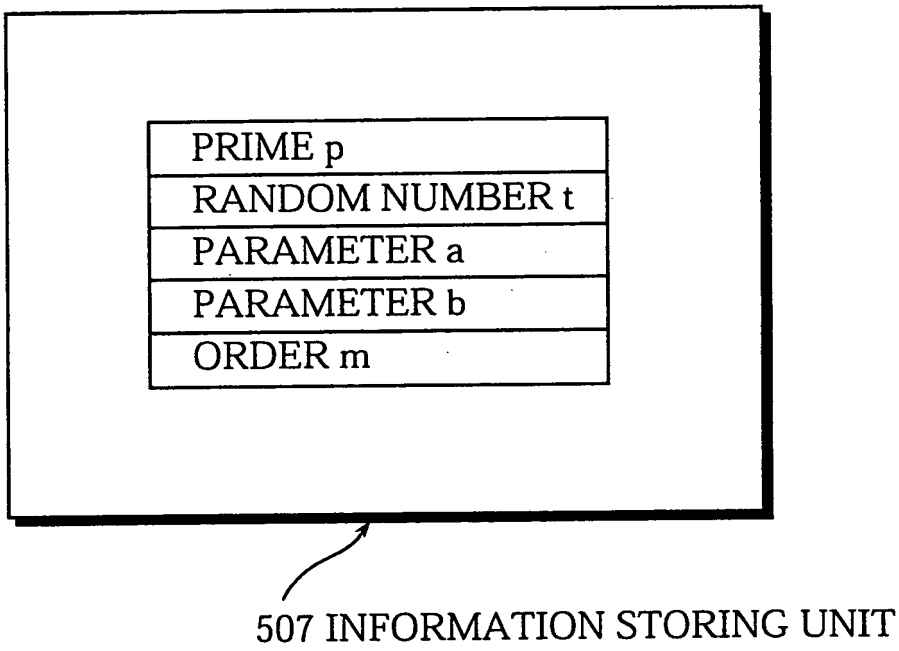

PRIME p
RANDOM NUMBER t
PARAMETER a
PARAMETER b
ORDER m
507 INFORMATION STORING UNIT

FIG. 7

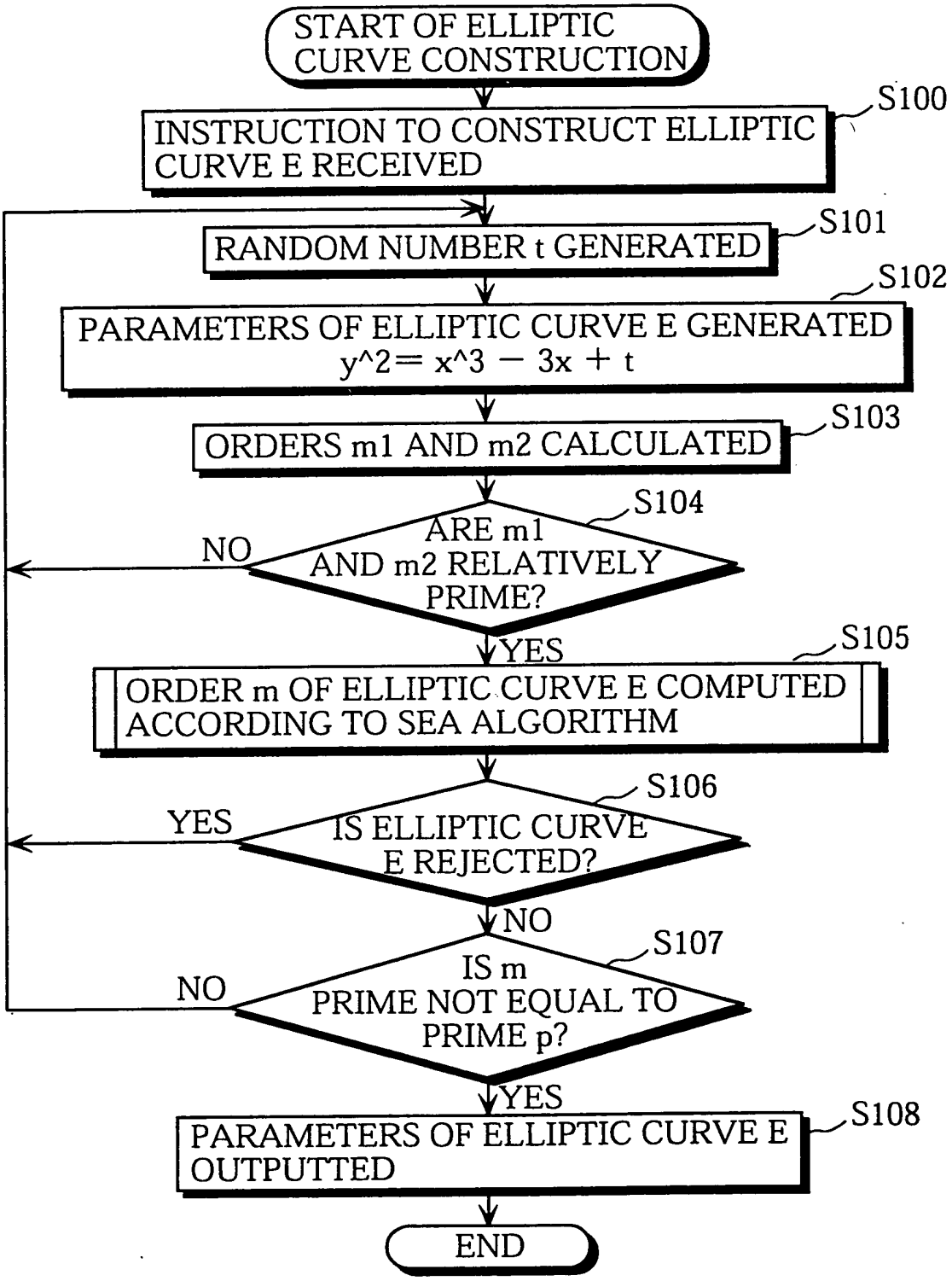

START OF ELLIPTIC CURVE CONSTRUCTION
INSTRUCTION TO CONSTRUCT ELLIPTIC CURVE E RECEIVED
S100
RANDOM NUMBER t GENERATED
S101
PARAMETERS OF ELLIPTIC CURVE E GENERATED
y^2= x^3 − 3x + t
S102
ORDERS m1 AND m2 CALCULATED
S103
ARE m1 AND m2 RELATIVELY PRIME?
S104
NO
YES
ORDER m OF ELLIPTIC CURVE E COMPUTED ACCORDING TO SEA ALGORITHM
S105
IS ELLIPTIC CURVE E REJECTED?
S106
YES
NO
IS m PRIME NOT EQUAL TO PRIME p?
S107
NO
YES
PARAMETERS OF ELLIPTIC CURVE E OUTPUTTED
S108
END

FIG. 8

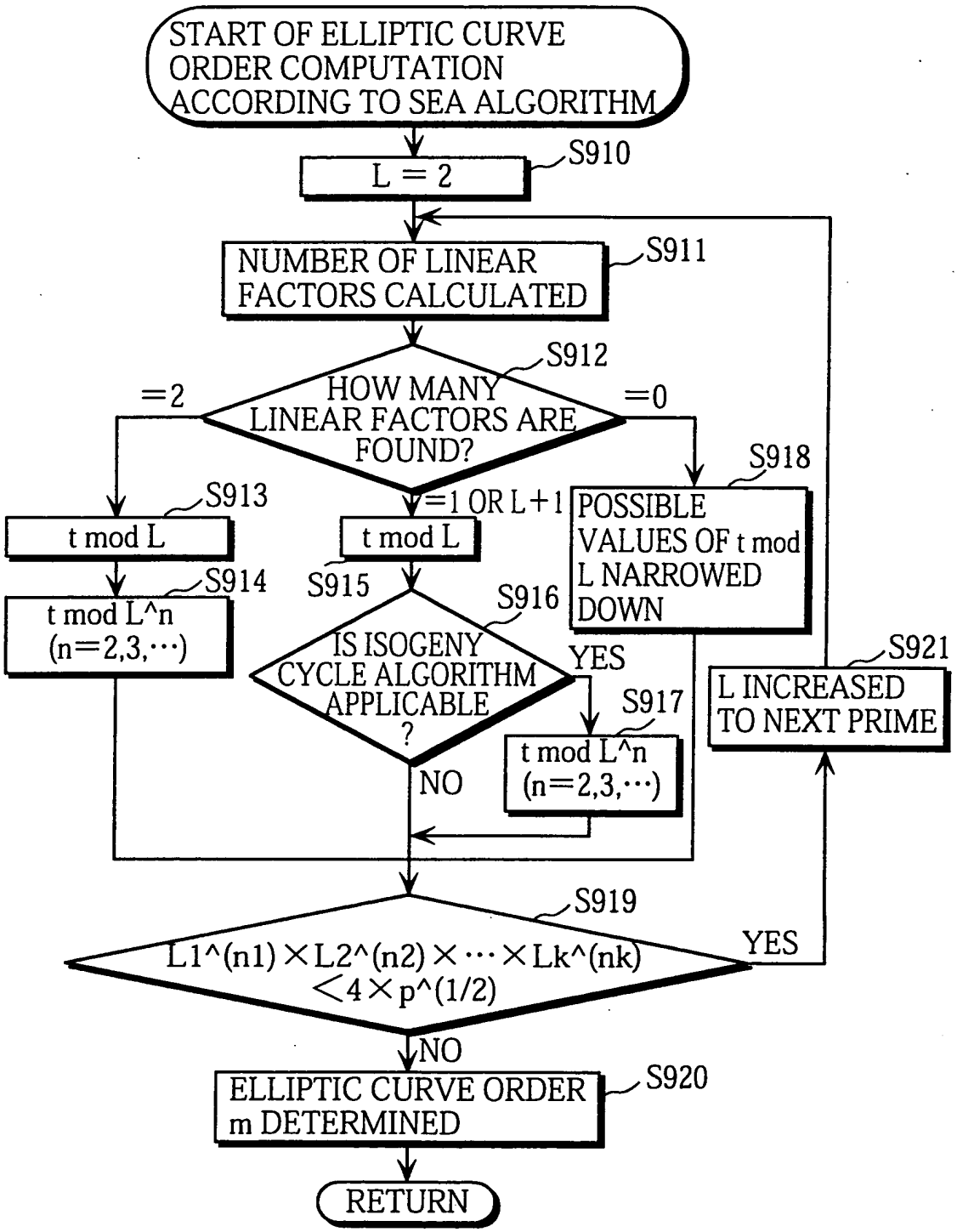

START OF ELLIPTIC CURVE ORDER COMPUTATION ACCORDING TO SEA ALGORITHM
L = 2
S910
NUMBER OF LINEAR FACTORS CALCULATED
S911
HOW MANY LINEAR FACTORS ARE FOUND?
S912
=2
=1 OR L+1
=0
t mod L
S913
t mod L^n (n=2,3,…)
S914
t mod L
S915
IS ISOGENY CYCLE ALGORITHM APPLICABLE ?
S916
YES
NO
t mod L^n (n=2,3,…)
S917
POSSIBLE VALUES OF t mod L NARROWED DOWN
S918
L INCREASED TO NEXT PRIME
S921
L1^(n1)×L2^(n2)×…×Lk^(nk) <4×p^(1/2)
S919
YES
NO
ELLIPTIC CURVE ORDER m DETERMINED
S920
RETURN

FIG. 9

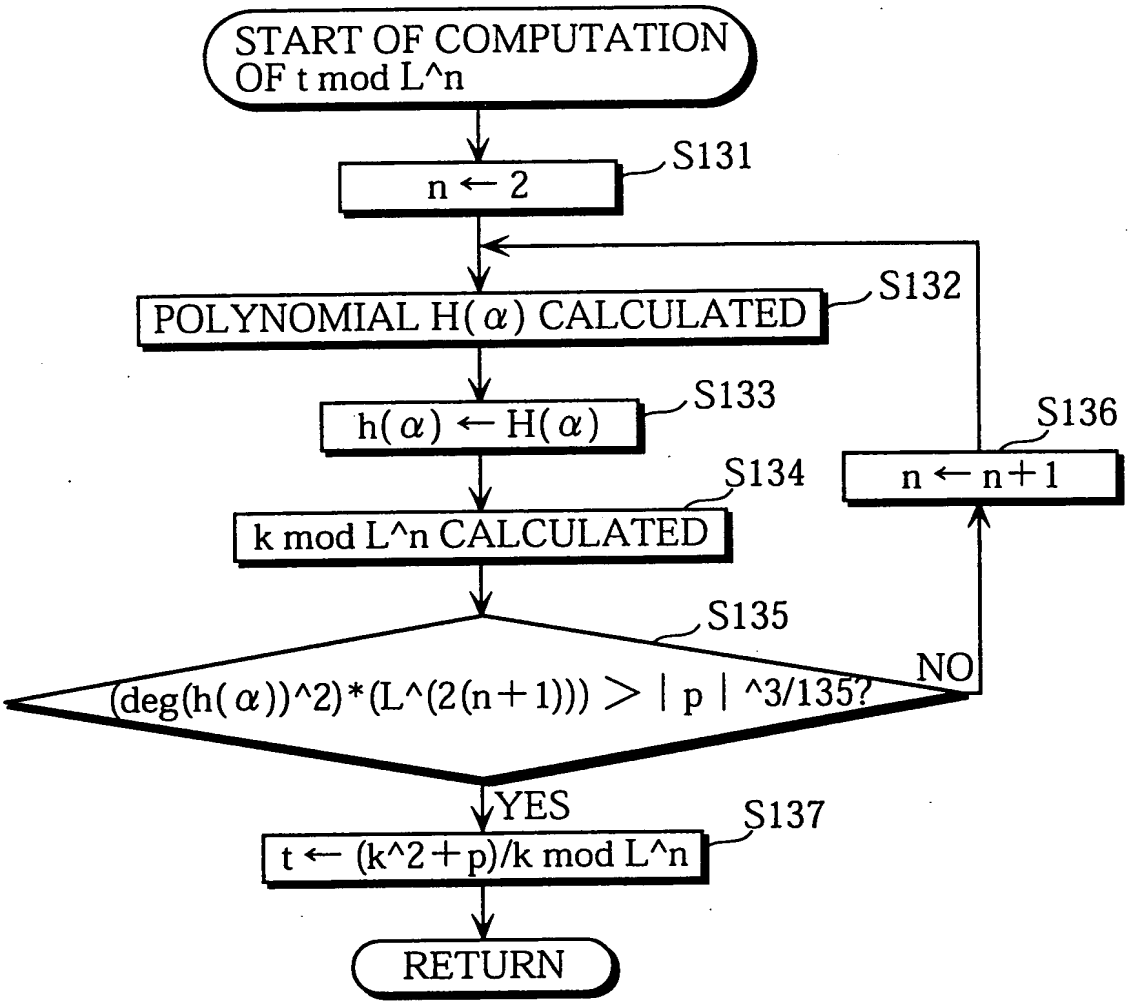
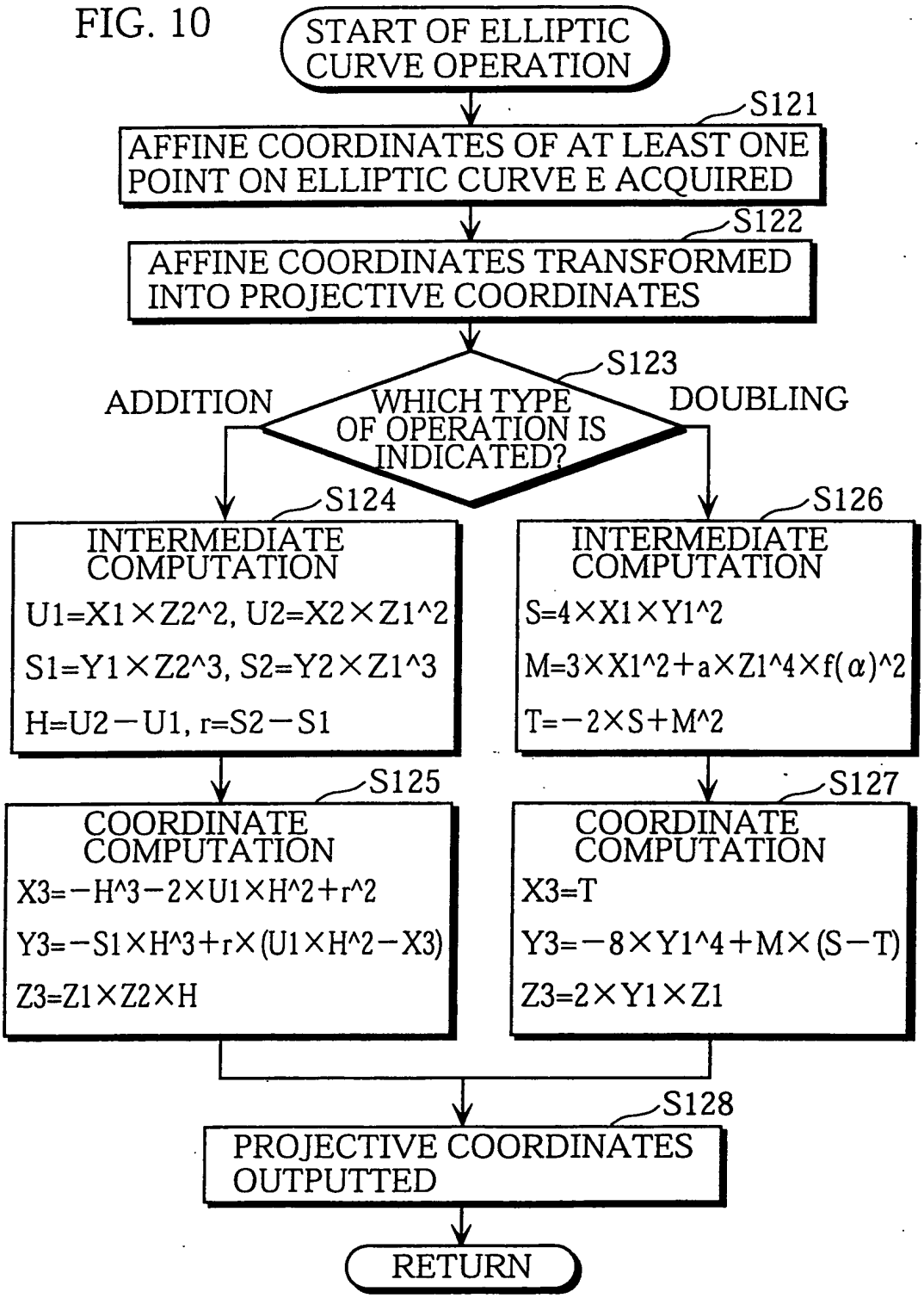

START OF COMPUTATION OF t mod L^n
n ← 2
S131
POLYNOMIAL H(α) CALCULATED
S132
h(α) ← H(α)
S133
k mod L^n CALCULATED
S134
(deg(h(α))^2)*(L^(2(n+1))) > | p | ^3/135?
S135
NO
n ← n+1
S136
YES
t ← (k^2+p)/k mod L^n
S137
RETURN

FIG. 10


START OF ELLIPTIC CURVE OPERATION
S121
AFFINE COORDINATES OF AT LEAST ONE POINT ON ELLIPTIC CURVE E ACQUIRED
S122
AFFINE COORDINATES TRANSFORMED INTO PROJECTIVE COORDINATES
S123
ADDITION
WHICH TYPE OF OPERATION IS INDICATED?
DOUBLING
S124
INTERMEDIATE COMPUTATION
U1=X1×Z2^2, U2=X2×Z1^2
S1=Y1×Z2^3, S2=Y2×Z1^3
H=U2−U1, r=S2−S1
S126
INTERMEDIATE COMPUTATION
S=4×X1×Y1^2
M=3×X1^2+a×Z1^4×f(α)^2
T=−2×S+M^2
S125
COORDINATE COMPUTATION
X3=−H^3−2×U1×H^2+r^2
Y3=−S1×H^3+r×(U1×H^2−X3)
Z3=Z1×Z2×H
S127
COORDINATE COMPUTATION
X3=T
Y3=−8×Y1^4+M×(S−T)
Z3=2×Y1×Z1
S128
PROJECTIVE COORDINATES OUTPUTTED
RETURN